REMARKS

Claims **55-74** are pending in the application.

Claims **55-74** stand rejected.

Claims **55, 65, and 70** have been amended.

Rejection of Claims under 35 U.S.C. §101

Claims 55, 65 and 70 stand rejected under 35 U.S.C. § 101. The Office action states that "the claimed subject matter is merely manipulating / generating an access control list...." (Page 2 of the 4/10/2007 Office Action). The Office Action also states that a useful, concrete, and tangible result is lacking and therefore the claimed invention is not patentable. Applicant respectfully traverses the rejection of these claims, particularly in light of the amendments made thereto.

Applicant respectfully asserts that generating an access control list comprising a destination user group identifier is useful and produces a tangible result, namely an access control list (ACL) containing a destination user group identifier. The result (i.e., an ACL populated (at least partially) with destination user group identifiers) can then applied in a practical manner. The ACL populated with a destination user group identifier is used to determine access permissions between network devices based on source and destination user groups. See, e.g., Applicant's Specification Par. 037, "Once the source and destination groups have been determined, the permissions (ACL) can be applied using this information." The usefulness of an ACL produced according to the claimed invention is further illustrated at least in Par. 007 of Applicant's specification, "[A] mechanism which allows for the efficient identification of network traffic...[S]uch an approach should employ existing ACL technology,

while reducing or eliminating the problem of multiplicative ACL growth that is currently encountered...." Accordingly, Claims 55, 65, and 70 recite statutory subject matter.

Claims 65-69 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant has amended claim 65, per Examiner's suggestion, for the sake of clarity, from "a computer readable medium" to "a computer readable storage medium." Applicant asserts that such amendment fully answers Examiner's rejection and respectfully requests that Examiner withdraw the rejection.

Rejection of Claims under 35 U.S.C. §102

Claims 55-60, 62, 63, 65-68 and 70-73 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Shannon, et al., U.S. Patent No. 6,233,618 (Shannon). Applicant respectfully disagrees.

While not conceding that the cited reference qualifies as prior art, but instead to expedite prosecution, Applicant has chosen to overcome this rejection by amendment. Applicant reserves the right, for example, in a continuing application, to establish that the cited reference does not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed.

Claim 55 has been amended to read:

A method comprising:

populating an access control list with a destination user group identifier, wherein said destination user group identifier identifies a destination user group of a destination,

said access control list comprises a source user group field configured to store a source user group identifier and a destination user group field configured to store a destination user group identifier,

said source user group comprises a plurality of source network devices,

said destination user group comprises a plurality of destination network devices, and

said access control list is configured to allow said source user group identifier and said destination user group identifier to be compared.

As discussed more fully below, nowhere does Shannon teach or disclose at least the following limitations: populating an access control list with a destination user group (DUG) identifier wherein said destination user group identifier identifies a destination user group of a destination; an access control list comprising a destination user group field configured to store a destination user group identifier; a destination user group comprising a plurality of destination network devices; or that the ACL is configured to allow the source user group (SUG) identifier and destination group identifier to be compared. Therefore, Applicant respectfully asserts that the cited reference fails to anticipate the claimed invention.

Shannon does not teach the claim limitation "populating an access control list with a destination user group identifier wherein said destination user group identifier identifies a destination user group of a destination."

The Office Action states that "[T]he group/category restricted destination database (as in Table 2) is qualified as an access control list with a destination user group identifier as a destination category identifier..." (Page 4 of the 4/10/2007 Office Action) Applicant respectfully disagrees. Claim 55 discloses a destination user group identifier. This is significantly different from the type of organizational grouping taught by Shannon. Shannon's categories cannot fairly be called user groups, and indeed, are not so called anywhere in the cited reference. Instead, each of the categories disclosed in Shannon typically represents a list of websites which contain content having a common theme or topic. From the abstract of Shannon, "limit[ing] to information content" is the heart of Shannon's invention. Therefore it is to be expected that "destinations" (typically website addresses) are categorized based on content located at that address. That way, access to information which is inappropriate or undesirable based on the type of information can be blocked. Doing so is the main thrust of Shannon. Shannon has nothing to do with the objectives of the claimed invention, which include using user groups to, for example, improve network security, allow scalability and manageability of changing network topologies when providing such improved security, help prevent ACLs from exploding to unwieldy size and so on. Therefore, it is unsurprising that Shannon fails to teach populating an ACL with a destination user group identifier wherein said destination user group identifier identifies a destination user group of a destination.

Shannon does not teach the claim limitation "an access control list comprising a destination user group field configured to store a destination user group identifier."

The category field in Shannon, i.e., the second column of Table 2, cannot fairly be characterized as a destination user group field. Instead, the category field of Table 2 contains a list of restricted categories and "other access attributes," such as days of the week and times of the day when access is restricted. The destination user group field in the presently claimed invention do not contain such "other access attributes." Shannon is directed to blocking access to a particular piece of information, based on the content of that information. Therefore, a particular host (server) could have several different pieces of information represented, for example, by several different URL addresses. Since Shannon's access control is based on the content of the information, for example alcohol related content, some of the URL's on a server may be allowed, and some blocked. Thus, other attributes may become relevant, and so it may become desirable to include such other attributes in the category field of Shannon's Table 2.

In contrast, the claimed invention restricts access to a host based on the user group that host is assigned to, and not on the type of information being requested from that host. For example, for a given destination user, the claimed invention would have no need to allow access to one file or folder and deny access to another. The relevant question is what group that destination belongs to. Therefore, no "other access information" is required in the destination user group field. The destination user group field is configured to store the destination user group identifier. Since Shannon does not disclose a field configured to store a destination user group identifier, Shannon cannot teach this element of the claimed invention.

Shannon does not teach the claim limitation "a destination user group comprising a plurality of destination network devices."

While Applicant does not concede that Shannon teaches destination user groups, if the categories taught by Shannon were to ever be capable of consideration as user groups (which Applicant specifically maintains they cannot), they would not and could not be comprised of destination network devices. The "destinations" referred to in Shannon are simply addresses where data may be found. For example, Shannon teaches a category database which comprises "IP addresses...which indicate which addresses of files, documents, web pages, web sites, and other information on the network...are restricted for access..." (Shannon: Column 8 Line 58-61). Again, the basis used by Shannon is content, not group membership. Further illustration of the patentably significant difference between the destination user groups comprising a plurality of destination network devices claimed in the present invention and the categories taught by Shannon is found in Shannon, Column 10 Line 8-11, "the location of any type of content on a computer network...Thus, each time the address of a content server is obtained or discovered by the network walker..." Thus, it is apparent that Shannon does not teach user groups comprising destination network devices.

Shannon does not teach the claim limitation "the capability to compare a source user group identifier and destination group identifier."

In the claimed invention, once the ACL is populated with the DUG identifier for a particular destination, the SUG identifier of a given packet and the DUG identifier of the

destination of that packet may be compared using this information as stored in the ACL. The comparison of each SUG-DUG pair yields information that ultimately indicates whether to allow or deny access to the destination, and so the handling of the given packet. By contrast, in Shannon, with respect to the comparisons that are made, the destination of a packet is compared against a list of prohibited destinations. At no time are a source group and a destination group compared. Thus, the inquiry in Shannon is not concerned with the source, but with the possible destinations that might be requested once again, based on their content.

Therefore, since Shannon does not teach the limitations discussed above, Shannon cannot anticipate Claim 55. Claims 65 and 74 have been amended similarly to claim 55. Since claims 65 and 74 contain limitations not found in Shannon, Shannon does not anticipate Claim 65 or 74. Applicant respectfully requests that Examiner withdraw the §102 rejection of Claims 55, 65, and 70.

Applicant further respectfully submits that dependent Claims 56-60, 62, 63, 66-68 and 71-73 are allowable as depending upon allowable base claims in addition to being allowable for various other reasons. Therefore Applicant respectfully requests that the § 102 rejections of those claims be withdrawn.

Rejection of Claims under 35 U.S.C. §103

Claims 61, 64, 69 and 74 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over by Shannon, et al., U.S. Patent No. 6,233,618 (Shannon), in view of Li, U.S. Patent No. 6,711,172 (Li). Applicant respectfully traverses this rejection.

In order for a claim to be rendered invalid under 35 U.S.C. § 103, the subject matter of the claim as a whole would have to be obvious to a person of ordinary skill in the art at the time the invention was made. *See* 35 U.S.C. § 103(a). This requires: (1) the reference(s) must teach or suggest all of the claim limitations; (2) there must be some teaching, suggestion or motivation to combine references either in the references themselves or in the knowledge of the art; and (3) there must be a reasonable expectation of success. *See* MPEP 2143; MPEP 2143.03; *In re Rouffet*, 149 F.3d 1350, 1355-56 (Fed. Cir. 1998)

While not conceding that the cited references qualify as prior art, but instead to expedite prosecution, Applicant has chosen to respectfully disagree and overcome this rejection thereby. Applicant reserves the right, for example, in a continuing application, to establish that the cited references do not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed. Applicant respectfully submits that Claims 61, 64, 69 and 74 are allowable over the cited references for at least the reasons discussed below.

More specifically, Applicant respectfully submits that neither Shannon nor Li, alone or in permissible combination show, teach, or suggest each element of Claim 61. Examiner correctly notes that Shannon does not teach a source group identifier stored in said packet. (Page 8 of the 4/10/2007 Office Action). This is unsurprising since Shannon is not directed to providing network security employing user groups such as those claimed. Instead, Shannon is directed to restricting access to certain content-based categories of information generally located on the Internet.

Shannon teaches a system where access to certain Internet information is controlled by a software program installed in a network gateway device. In Shannon, when a request for Internet information is sent from a source and received at the network gateway device, the software

determines (i.e., looks up in a database) to which group the requesting source belongs and which categories of information are restricted for that group. If the request is allowable, i.e., the content of the destination has resulted in the destination not being included in the category/destination database, the network gateway device allows the request to proceed to the Internet.

One of the shortcomings Shannon's system specifically intends to address is the situation in which installing access control software on a computer for which access is being restricted increases the risk that users of that computer will find it possible to disable the access control software. To overcome this problem, Shannon installs its system on a network gateway device. This gateway device has access to a group/source database which contains destinations that contain inappropriate content. In order to store identifying information in a packet, either the source would have to be allowed access to the source/group database, and have the capability to rewrite packets being sent, or the network gateway device would have to do it.

The former course is not shown, taught, or suggested in any way by Shannon. In fact, Shannon teaches away from allowing individual source computers access to the group/source database. This is intuitively consistent since allowing individuals access to the group/category database would run counter to the express purpose of reducing the likelihood that a user will be able to circumvent the system and so access inappropriate content.

The latter, i.e., having the gateway device rewrite the request packet, would serve no purpose whatsoever in Shannon's system, and would simply be a performance drain with no benefit. Having the network gateway rewrite packets to include source group information would involve the following steps: the gateway device receiving a packet (request for Internet information); determining the packet's source; looking up the packet source's group in the source/group database; and then adding the group to the packet. Presumably the gateway device

would then need to extract the source group from the packet, determine which categories are restricted for that source group, and proceed with determining whether the request is allowable. It can be seen that the steps of adding the group to the packet and then extracting the source group is extra processing with no apparent purpose, and would even be useless. Eliminating extraneous steps or processes is simply the definition of efficiency. Conversely, adding unnecessary steps which provide no benefit is wasteful and inefficient. Further, since all group based access control in Shannon's system is performed before a packet is sourced onto a WAN, there is simply no need to embed any such information in a packet in Shannon's system. Having the packet carry along its source group identifier after passing through the network gateway device would require additional bits in the packet, and once the packet has passed through the network gateway device, Shannon does not teach any scenario in which those bits would or could ever again be considered.

The Office Action states that Li teaches "a source user group identifier stored in said packet." (Page 8 of the 4/10/2007 Office Action) However, Applicant respectfully asserts that the Office Action misstates the nature of the information stored in the packet. There is no source user group taught or suggested anywhere in Li. Li discloses a method of more efficiently routing network traffic, principally multicast traffic, from a given source to members of an intended recipient group, using lookup tables for intermediate routers. The lookup tables facilitate finding the shortest path between the source and the members of the group that the source is broadcasting to. In so doing, Li creates a source/group pair based on information extracted from the packets being routed. However, the group referred to is a multicast group address, not a group of sources. The "source" part of the term "source/group" as used in Li refers to a singular sender, and the "group" part refers to a recipient multicast group. Again, Li does not teach or

suggest any grouping of source users. This makes sense since Li is directed to minimizing a packet's travel time between networks, and is not directed to providing network security employing user group-based access control lists, such as the claimed invention.

Based on the above discussion, Applicant respectfully asserts that neither Shannon nor Li provides any motivation to combine their disclosures, and one of skill in the art at the time of invention would not have been so motivated, based on their disclosures and/or that person's skill in the art. The method disclosed in Li of routing packets to border routers involves routers updating lookup tables with addresses and ranges of addresses to determine whether packets should be sent to a rendezvous point (RP), if so which one, or if they can bypass the RP and be forwarded to border routers. There is no suggestion that adding Shannon's source grouping and prohibiting certain groups of sources from accessing certain categories of websites would enhance Li's method in any way. Likewise, there is no suggestion that adding the method of Li, with its RP sets and state based forwarding tables, to Shannon would provide any advantage whatsoever.

In fact, attempting to do so would add a level of cost and complexity far beyond what might be envisioned by one of ordinary skill in the art, were such a person tasked with such a project. Shannon "knows" which sites are restricted by means of a human editor evaluating sites which are collected as the sites come online. The (human) editor then makes a determination about the site's content. Periodically, the editor updates the category/restricted destination database and then a user (subscriber) of Shannon's system downloads the updated database. It is clear that this process of updating the database takes significant periods of time; likely on the scale of days, weeks, or even months. Such "processing" is far too slow to utilize the system disclosed in Li. Li's system makes decisions about packet routing "during periods of high

network traffic" to alleviate congestion. These decisions and changes in routing are much more dynamic in nature. Waiting days for a subscriber to update their category/restricted destination database simply wouldn't work with Li, which is making decisions based on improving performance more likely on the order of nano- or micro-seconds.

Additionally, if Li and Shannon could be combined, which Applicant maintains is not possible, adding Li to Shannon would not improve Shannon in any way. The object of Shannon is to limit access to certain categories of information content. Speeding up multicast packet transmission is simply irrelevant to accomplishing this objective. While faster network data transmission is desirable, of course, that is not Shannon's goal.

Conversely, Li's routing decisions have nothing to do with content. Li determines what resources are using a rendezvous point and if that RP can be bypassed. Again, the making of such a determination is completely oblivious to content of the resources in question. Throwing out the window any awareness of content surely cannot be considered an improvement to Shannon's system of content-based access limitation. Therefore Applicant respectfully asserts that one of skill in the art at the time of invention would not have been motivated to combine the disclosures of Shannon and Li.

Moreover, even if the category-based Internet information access program were combined with the multicast network packet forwarding method, which Applicant maintains one of skill in the art at the time of invention would not have been motivated to do, the disclosures could not be combined in the manner suggested in the Office Action, and even if combined, such a combination would not, and could not, function properly. Shannon does not disclose the hardware necessary to define and utilize forwarding tables for rendezvous points for forwarding packets to border routers. Shannon simply consults a database for a list of addresses and

compares them to addresses stored in a packet. Shannon's system operates exclusively in a domain which is bounded by the gateway network device. Shannon's system completes its function before any packets exit the domain bounded by the network gateway device and enter another domain, typically the Internet (see Shannon: Figure 1.) Li, on the other hand, is concerned with routing packets between domains. This requires knowledge not only about the network on one side of a router, but also on the other side. Li's system utilizes information not only about the source of a packet, but about the packet's path towards a destination, i.e., the RP it is destined for and beyond that, ultimately the recipient the packet is bound for. This knowledge, collected in forwarding tables, allows Li's system to make smart decisions about how to route the packet. Shannon's system discloses no such information or awareness capabilities. Shannon's system simply determines whether to allow a request to pass through the network gateway device. At that point, it has been determined that the content being requested is allowable, and Shannon's system has completely satisfied the stated purpose of limiting access to certain information content.

Further, neither Shannon nor Li, alone or in combination, would solve the problems addressed by the instant invention. For example, employing user groups to provide enhanced network security while preventing multiplicative ACL growth is not a beneficial result that such a combination would or even could contemplate. This makes sense since neither Shannon nor Li is directed toward solving anything remotely related to such a problem. Shannon is directed to limiting access to certain information on the Internet, and Li is directed to routing packets to border routers between domains based on address-based forwarding tables. Even if an ill-advised attempt was made to use the cited references to solve the problems solved by the instant invention, since the cited references do not include all elements taught in the claimed invention,

either alone or in permissible combination, there is no likelihood that any permissible combination would be successful in doing so. For the reasons presented above, neither Shannon nor Li, alone or in combination, teaches a source user group identifier stored in a packet, as taught by Claim 61.

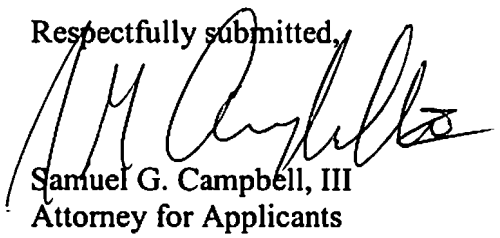
Regarding claims 64, 69, and 74, as Examiner correctly notes, Shannon does not teach the limitation of extracting a source user group identifier from a packet. The Office Action states that Li does teach extracting a source user group identifier from a packet. Applicant respectfully disagrees. As discussed above, Li makes no mention of a source user group at all, much less extracting one from a packet. For at least this reason, as well as those presented above, neither Shannon nor Li, alone or in combination, teaches extracting a source user group identifier from a packet, as taught by Claims 64, 69, and 74.

In light of the foregoing arguments and amendments, Shannon fails to anticipate the claimed invention as claimed in independent claims 55, 65, and 70. Further, in light of the foregoing arguments, Shannon and Li, taken alone or in permissible combination, even in light of skill in the art (which Applicant maintains is neither appropriate nor properly defined in the Office Action), fail to make obvious the claimed invention, as claimed in claims 61, 64, 69, and 74. Moreover, Applicant respectfully asserts that claims 56-64, 66-68, and 71-74 which depend from independent claims 55, 65, and 70, respectively, are also allowable, for at least the foregoing reasons.

CONCLUSION

In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned at 512-439-5084.

Respectfully submitted,



Samuel G. Campbell, III
Attorney for Applicants
Reg. No. 42,381
Telephone: (512) 439-5084
Facsimile: (512) 439-5099